

# COLLUSIONS IN TEICHMÜLLER EXPANSIONS

TREVOR HYDE

ABSTRACT. If  $\mathfrak{p} \subseteq \mathbb{Z}[\zeta]$  is a prime ideal over  $p$  in the  $(p^d - 1)$ th cyclotomic extension of  $\mathbb{Z}$ , then every element  $\alpha$  of the completion  $\mathbb{Z}[\zeta]_{\mathfrak{p}}$  has a unique expansion as a power series in  $p$  with coefficients in  $\mu_{p^d-1} \cup \{0\}$  called the *Teichmüller expansion* of  $\alpha$  at  $\mathfrak{p}$ . We observe three peculiar and seemingly unrelated patterns that frequently appear in the computation of Teichmüller expansions, then develop a unifying theory to explain these patterns in terms of the dynamics of an affine group action on  $\mathbb{Z}[\zeta]$ .

## 1. INTRODUCTION

Let  $p$  be a prime,  $q = p^d$  a power of  $p$ , and let  $\zeta$  be a primitive  $(q - 1)$ th root of unity. For any prime ideal  $\mathfrak{p} \subseteq \mathbb{Z}[\zeta]$  over  $p$ , we have an isomorphism  $\mathbb{Z}[\zeta]/\mathfrak{p} \cong \mathbb{F}_q$ . Let  $\rho : \mathbb{Z}[\zeta] \rightarrow \mathbb{F}_q$  be the reduction modulo  $\mathfrak{p}$  map. We call a section  $\tilde{\tau} : \mathbb{F}_q \rightarrow \mathbb{Z}[\zeta]$  of  $\rho$  a *lift*. Given a lift  $\tilde{\tau}$ , there is a unique way to expand any element of the completion  $\mathbb{Z}[\zeta]_{\mathfrak{p}}$  as a power series in  $p$  with coefficients in  $\tilde{\tau}(\mathbb{F}_q)$ .

While there are many lifts of  $\rho$ , there is a unique *multiplicative lift*  $\tau$  called the *Teichmüller lift* [2, Chp. XII, Exer. 16]. Let  $\mu_{q-1}$  denote the multiplicative group of  $(q - 1)$ th roots of unity. Since  $q - 1$  is coprime to  $p$ , the reduction map  $\rho$  restricts to an injective group homomorphism  $\rho : \mu_{q-1} \rightarrow \mathbb{F}_q^\times$ . Extending the restriction to include 0 we see that  $\rho : \mu_{q-1} \cup \{0\} \rightarrow \mathbb{F}_q$  is an isomorphism of multiplicative monoids. The Teichmüller lift  $\tau$  is defined as the inverse of this isomorphism, hence is multiplicative. Because  $\tau$  is the unique multiplicative lift,  $\tau(\mathbb{F}_q)$  can be seen as a canonical set of coefficients with which to expand elements of  $\mathbb{Z}[\zeta]_{\mathfrak{p}}$ . We refer to the expansion of an element  $\alpha \in \mathbb{Z}[\zeta]_{\mathfrak{p}}$  with respect to  $\tau$  as the *Teichmüller expansion* of  $\alpha$ .

The extension of complete local rings  $\mathbb{Z}[\zeta]/\mathbb{Z}_p$  has degree  $d$  where  $q = p^d$  and is unramified. There is a unique unramified extension of  $\mathbb{Z}_p$  of each degree  $d$  up to isomorphism [5, Thm. 3], hence  $\mathbb{Z}[\zeta]_{\mathfrak{p}}$  provides a model. Teichmüller expansions give a formal way to construct this unique extension of  $\mathbb{Z}_p$  in terms of  $\mathbb{F}_q$  alone; these are the  $p$ -typical Witt vectors  $W_p(\mathbb{F}_q)$  [5, Chp. 2 §6]. More generally, Teichmüller lifts are essential to the construction of the big Witt vectors  $W(A)$  for any commutative ring  $A$  [1]. Thus one reason to be interested in Teichmüller expansions is to understand the ring structure of Witt vectors  $W_p(\mathbb{F}_q) \cong \mathbb{Z}[\zeta]_{\mathfrak{p}}$ . The elements of  $\mathbb{Z}[\zeta]_{\mathfrak{p}}$  may be written as power series in  $p$  with coefficients in  $\tau(\mathbb{F}_q)$ . Our coefficients are closed under multiplication—this is the characteristic property of the Teichmüller lift  $\tau$ —but are not closed under addition. The additive structure is complicated by “carrying.” Hence we need to compute the Teichmüller expansions of  $\zeta^a + \zeta^b$  in order to do arithmetic in  $\mathbb{Z}[\zeta]_{\mathfrak{p}}$ .

Teichmüller expansions are laborious to compute by hand and in the case  $q = p$  are less convenient than the usual expression of elements as power series in  $p$  with integral coefficients  $0 \leq i < p$ . The difficulty is circumvented with the help of a machine. Peculiar patterns frequently arise as one computes Teichmüller expansions. In this paper we observe three seemingly unrelated

phenomena and develop a unifying theory to explain them in terms of the dynamics of an affine group action on the global ring  $\mathbb{Z}[\zeta]$ .

We collect our observations in Section 2, followed by a review of cyclotomy in Section 3. We obtain results in Section 4 and apply them to explain our examples in Section 5.

## 2. OBSERVATIONS

Recall that  $p$  is a prime,  $q = p^d$  is a power of  $p$ , and  $\zeta$  is a primitive  $(q - 1)$ th root of unity. Given an element  $\alpha \in \mathbb{Z}[\zeta]$  and a prime ideal  $\mathfrak{p} \subseteq \mathbb{Z}[\zeta]$  over  $p$ , the *Teichmüller expansion of  $\alpha$  at  $\mathfrak{p}$*  is the unique series

$$\alpha = \tau(0, \alpha, \mathfrak{p}) + \tau(1, \alpha, \mathfrak{p})p + \tau(2, \alpha, \mathfrak{p})p^2 + \dots = \sum_{m \geq 0} \tau(m, \alpha, \mathfrak{p})p^m \in \mathbb{Z}[\zeta]_{\mathfrak{p}},$$

such that  $\tau(m, \alpha, \mathfrak{p}) \in \tau(\mathbb{F}_q) = \mu_{q-1} \cup \{0\}$  for each  $m \geq 0$ . The  $\tau(m, \alpha, \mathfrak{p})$  are called *Teichmüller coefficients of  $\alpha$  at  $\mathfrak{p}$* .

To compute explicit Teichmüller expansions we must first choose a prime  $\mathfrak{p}$  over  $p$  in  $\mathbb{Z}[\zeta]$ . The Kummer-Dedekind theorem [4, Chp 1, 8.3] says that

$$\mathfrak{p} = (p, f(\zeta)) \subseteq \mathbb{Z}[\zeta]$$

where  $f(x) \in \mathbb{Z}[x]$  is congruent modulo  $p$  to an irreducible factor of the cyclotomic polynomial  $\Phi_{q-1}(x)$  in  $\mathbb{Z}_p[x]$ . There are  $\varphi(q - 1)/d$  such irreducible factors of degree  $d$ .

For the moment, let  $q = p^d = 2^4$  and let  $\zeta$  be a  $q - 1 = 15$ th root of unity. The cyclotomic polynomial

$$\Phi_{15}(x) = x^8 - x^7 + x^5 - x^4 + x^3 - x + 1$$

factors into a product of  $\varphi(q - 1)/d = \varphi(15)/4 = 2$  degree 4 irreducible polynomials over  $\mathbb{Z}_2$  whose reductions modulo 2 are:

$$\begin{aligned} f_1(x) &\equiv x^4 + x + 1 \pmod{2} \\ f_2(x) &\equiv x^4 + x^3 + 1 \pmod{2}. \end{aligned}$$

Let  $\mathfrak{p}_i := (2, f_i(\zeta))$ .

Below are examples of Teichmüller expansions at  $\mathfrak{p}_1$  of sums of two distinct roots of unity.

$$\begin{aligned} \zeta^0 + \zeta^1 &= \zeta^4 + \zeta^8 p + \zeta^6 p^2 + \zeta^5 p^3 + \zeta^3 p^4 + 0 p^5 + \zeta^8 p^6 + \zeta^{10} p^7 + \zeta^7 p^8 + \zeta^{10} p^9 + \dots \\ \zeta^1 + \zeta^3 &= \zeta^9 + \zeta^2 p + \zeta^{13} p^2 + \zeta^{11} p^3 + \zeta^7 p^4 + 0 p^5 + \zeta^2 p^6 + \zeta^6 p^7 + \zeta^0 p^8 + \zeta^6 p^9 + \dots \\ \zeta^2 + \zeta^{10} &= \zeta^4 + \zeta^6 p + \zeta^5 p^2 + \zeta^{12} p^3 + \zeta^{11} p^4 + 0 p^5 + \zeta^6 p^6 + \zeta^7 p^7 + \zeta^{13} p^8 + \zeta^7 p^9 + \dots \\ \zeta^3 + \zeta^7 &= \zeta^4 + \zeta^5 p + \zeta^{12} p^2 + \zeta^8 p^3 + \zeta^0 p^4 + 0 p^5 + \zeta^5 p^6 + \zeta^{13} p^7 + \zeta^1 p^8 + \zeta^{13} p^9 + \dots \end{aligned}$$

No apparent patterns emerge in the sequence of Teichmüller coefficients for an individual expansion. However, we do see some striking relationships between the expansions of different elements. First notice the conspicuous 0 appearing as the coefficient of  $p^5$  in each expansion. Continuing the expansions this phenomenon persists:

$$\begin{aligned} \zeta^0 + \zeta^1 &= \dots \zeta^2 p^{10} + \zeta^{11} p^{11} + \mathbf{0} p^{12} + \zeta^1 p^{13} + \zeta^{12} p^{14} + \zeta^7 p^{15} + \mathbf{0} p^{16} + \zeta^{14} p^{17} + \zeta^2 p^{18} + \dots \\ \zeta^1 + \zeta^3 &= \dots \zeta^5 p^{10} + \zeta^8 p^{11} + \mathbf{0} p^{12} + \zeta^3 p^{13} + \zeta^{10} p^{14} + \zeta^0 p^{15} + \mathbf{0} p^{16} + \zeta^{14} p^{17} + \zeta^5 p^{18} + \dots \\ \zeta^2 + \zeta^{10} &= \dots \zeta^3 p^{10} + \zeta^0 p^{11} + \mathbf{0} p^{12} + \zeta^{10} p^{13} + \zeta^8 p^{14} + \zeta^{13} p^{15} + \mathbf{0} p^{16} + \zeta^9 p^{17} + \zeta^3 p^{18} + \dots \\ \zeta^3 + \zeta^7 &= \dots \zeta^{11} p^{10} + \zeta^2 p^{11} + \mathbf{0} p^{12} + \zeta^7 p^{13} + \zeta^6 p^{14} + \zeta^1 p^{15} + \mathbf{0} p^{16} + \zeta^{14} p^{17} + \zeta^{11} p^{18} + \dots \end{aligned}$$

Looking closer we see the coefficients of  $p^7$  and  $p^9$  match in each expansion

$$\begin{aligned}\zeta^0 + \zeta^1 &= \dots \zeta^{10} p^7 + \zeta^7 p^8 + \zeta^{10} p^9 + \dots \\ \zeta^1 + \zeta^3 &= \dots \zeta^6 p^7 + \zeta^0 p^8 + \zeta^6 p^9 + \dots \\ \zeta^2 + \zeta^{10} &= \dots \zeta^7 p^7 + \zeta^{13} p^8 + \zeta^7 p^9 + \dots \\ \zeta^3 + \zeta^7 &= \dots \zeta^{13} p^7 + \zeta^1 p^8 + \zeta^{13} p^9 + \dots\end{aligned}$$

suggesting these expansions may actually be the same under a permutation of the coefficients. The table below supports this claim, showing distributions of the 16 digits in each of the four expansions up to 500 terms.

	0	$\zeta^0$	$\zeta^1$	$\zeta^2$	$\zeta^3$	$\zeta^4$	$\zeta^5$	$\zeta^6$	$\zeta^7$	$\zeta^8$	$\zeta^9$	$\zeta^{10}$	$\zeta^{11}$	$\zeta^{12}$	$\zeta^{13}$	$\zeta^{14}$
$\zeta^0 + \zeta^1$	5.4	7.6	7.0	6.2	5.6	5.6	7.4	5.2	5.0	5.4	5.8	8.4	7.8	4.4	6.8	6.4
$\zeta^1 + \zeta^3$	5.4	5.0	7.6	5.4	7.0	5.8	6.2	8.4	5.6	7.8	5.6	4.4	7.4	6.8	5.2	6.4
$\zeta^2 + \zeta^{10}$	5.4	7.8	6.8	7.6	6.2	5.6	5.2	5.4	8.4	4.4	6.4	7.0	5.6	7.4	5.0	5.8
$\zeta^3 + \zeta^7$	5.4	5.6	5.0	7.8	7.6	5.6	5.4	4.4	7.0	7.4	5.8	6.8	6.2	5.2	8.4	6.4

The rows are in fact permutations of one another with enough distinct entries to almost determine the bijection between them. Notice that the permutations appear to fix zero. We call this phenomenon the **permutation conspiracy**: seemingly unrelated elements of  $\mathbb{Z}[\zeta]$  having the same Teichmüller expansion up to a permutation of the coefficients fixing zero. We explain the permutation conspiracy in Section 5.

Not every Teichmüller expansion of  $\zeta^a + \zeta^b$  at  $\mathfrak{p}_1$  is a permutation of one seen above. Here are examples of periodic expansions:

$$\begin{aligned}\zeta^1 + \zeta^6 &= \zeta^{11} + \zeta^{11}p + \zeta^{11}p^2 + \zeta^{11}p^3 + \zeta^{11}p^4 + \zeta^{11}p^5 + \zeta^{11}p^6 + \zeta^{11}p^7 + \zeta^{11}p^8 + \zeta^{11}p^9 + \dots \\ \zeta^4 + \zeta^{14} &= \zeta^9 + \zeta^9p + \zeta^9p^2 + \zeta^9p^3 + \zeta^9p^4 + \zeta^9p^5 + \zeta^9p^6 + \zeta^9p^7 + \zeta^9p^8 + \zeta^9p^9 + \dots\end{aligned}$$

Note that the exponents on the left hand side differ by a multiple of 5 in each case.

The following expansions are related by a permutation conspiracy but also have **restricted coefficients** taken from the set  $\{0, \zeta^4, \zeta^9, \zeta^{14}\}$ .

$$\begin{aligned}\zeta^0 + \zeta^3 &= \zeta^{14} + \zeta^9p + \zeta^4p^2 + \zeta^9p^3 + \zeta^{14}p^4 + 0p^5 + 0p^6 + \zeta^9p^7 + \zeta^{14}p^8 + 0p^9 + \dots \\ \zeta^2 + \zeta^{11} &= \zeta^9 + \zeta^{14}p + \zeta^4p^2 + \zeta^{14}p^3 + \zeta^9p^4 + 0p^5 + 0p^6 + \zeta^{14}p^7 + \zeta^9p^8 + 0p^9 + \dots \\ \zeta^1 + \zeta^7 &= \zeta^{14} + \zeta^4p + \zeta^9p^2 + \zeta^4p^3 + \zeta^{14}p^4 + 0p^5 + 0p^6 + \zeta^4p^7 + \zeta^{14}p^8 + 0p^9 + \dots\end{aligned}$$

The exponents on the left hand side differ by multiples of 3 in each case.

How do we account for these special expansions with periodic or restricted coefficients? Can we predict when such phenomena will occur and what coefficients will appear? An affirmative answer is provided in Section 5.

Still working with  $q = 16$ , we now compare the Teichmüller expansions of an element at both of the primes  $\mathfrak{p}_1, \mathfrak{p}_2$  over  $p$ .

$$\mathfrak{p}_1 : \zeta^0 + \zeta^1 = \zeta^4 + \zeta^8 p + \zeta^6 p^2 + \zeta^5 p^3 + \zeta^3 p^4 + 0 p^5 + \zeta^8 p^6 + \zeta^{10} p^7 + \zeta^7 p^8 + \zeta^{10} p^9 + \dots$$

$$\mathfrak{p}_2 : \zeta^0 + \zeta^1 = \zeta^{12} + \zeta^8 p + \zeta^{10} p^2 + \zeta^{11} p^3 + \zeta^{13} p^4 + 0 p^5 + \zeta^8 p^6 + \zeta^6 p^7 + \zeta^9 p^8 + \zeta^6 p^9 + \dots$$

$$\mathfrak{p}_1 : \zeta^4 + \zeta^{14} = \zeta^9 + \zeta^9 p + \zeta^9 p^2 + \zeta^9 p^3 + \zeta^9 p^4 + \zeta^9 p^5 + \zeta^9 p^6 + \zeta^9 p^7 + \zeta^9 p^8 + \zeta^9 p^9 + \dots$$

$$\mathfrak{p}_2 : \zeta^4 + \zeta^{14} = \zeta^9 + \zeta^9 p + \zeta^9 p^2 + \zeta^9 p^3 + \zeta^9 p^4 + \zeta^9 p^5 + \zeta^9 p^6 + \zeta^9 p^7 + \zeta^9 p^8 + \zeta^9 p^9 + \dots$$

$$\mathfrak{p}_1 : \zeta^2 + \zeta^{11} = \zeta^9 + \zeta^{14} p + \zeta^4 p^2 + \zeta^{14} p^3 + \zeta^9 p^4 + 0 p^5 + 0 p^6 + \zeta^{14} p^7 + \zeta^9 p^8 + 0 p^9 + \dots$$

$$\mathfrak{p}_2 : \zeta^2 + \zeta^{11} = \zeta^4 + \zeta^{14} p + \zeta^9 p^2 + \zeta^{14} p^3 + \zeta^4 p^4 + 0 p^5 + 0 p^6 + \zeta^{14} p^7 + \zeta^4 p^8 + 0 p^9 + \dots$$

In each example, the product  $\tau(m, \alpha, \mathfrak{p}_1) \tau(m, \alpha, \mathfrak{p}_2)$  is independent of  $m$  whenever its nonzero. The values of the products are  $\zeta^1, \zeta^3, \zeta^{13}$  respectively (recall that  $\zeta$  is a 15th root of unity.) We refer to this relationship between the Teichmüller coefficients of  $\alpha$  at different primes as **prime collusion**.

To get a better sense of prime collusion, let us consider examples when  $q = p^d = 2^6$ . Then  $\zeta$  is a 63rd root of unity. The polynomial  $\Phi_{63}(x)$  factors into  $\varphi(63)/6 = 6$  degree 6 irreducible polynomials in  $\mathbb{Z}_2[x]$ .

$$\begin{array}{ll} g_1(x) \equiv x^6 + x^5 + x^4 + x + 1 \pmod{2} & g_2(x) \equiv x^6 + x + 1 \pmod{2} \\ g_3(x) \equiv x^6 + x^5 + x^3 + x^2 + 1 \pmod{2} & g_4(x) \equiv x^6 + x^4 + x^3 + x + 1 \pmod{2} \\ g_5(x) \equiv x^6 + x^5 + 1 \pmod{2} & g_6(x) \equiv x^6 + x^5 + x^2 + x + 1 \pmod{2} \end{array}$$

Let  $\mathfrak{p}_i = (2, g_i(\zeta))$ . Each element has 6 expansions, for instance:

$$\mathfrak{p}_1 : \zeta^0 + \zeta^1 = \zeta^{39} + \zeta^{32} p + \zeta^4 p^2 + \zeta^{53} p^3 + \zeta^{35} p^4 + \zeta^2 p^5 + \zeta^2 p^6 + \zeta^{44} p^7 + \zeta^{39} p^8 + \zeta^2 p^9 + \dots$$

$$\mathfrak{p}_6 : \zeta^0 + \zeta^1 = \zeta^{25} + \zeta^{32} p + \zeta^{60} p^2 + \zeta^{11} p^3 + \zeta^{29} p^4 + \zeta^{62} p^5 + \zeta^{62} p^6 + \zeta^{20} p^7 + \zeta^{25} p^8 + \zeta^{62} p^9 + \dots$$

$$\mathfrak{p}_2 : \zeta^0 + \zeta^1 = \zeta^6 + \zeta^{32} p + \zeta^{19} p^2 + \zeta^{44} p^3 + \zeta^1 p^4 + \zeta^{11} p^5 + \zeta^{24} p^6 + \zeta^{29} p^7 + \zeta^{20} p^8 + \zeta^{16} p^9 + \dots$$

$$\mathfrak{p}_5 : \zeta^0 + \zeta^1 = \zeta^{58} + \zeta^{32} p + \zeta^{45} p^2 + \zeta^{20} p^3 + \zeta^0 p^4 + \zeta^{53} p^5 + \zeta^{40} p^6 + \zeta^{35} p^7 + \zeta^{44} p^8 + \zeta^{48} p^9 + \dots$$

$$\mathfrak{p}_3 : \zeta^0 + \zeta^1 = \zeta^8 + \zeta^{32} p + \zeta^{20} p^2 + \zeta^{14} p^3 + \zeta^{51} p^4 + \zeta^{20} p^5 + \zeta^{40} p^6 + \zeta^{37} p^7 + \zeta^{40} p^8 + \zeta^{45} p^9 + \dots$$

$$\mathfrak{p}_4 : \zeta^0 + \zeta^1 = \zeta^{56} + \zeta^{32} p + \zeta^{44} p^2 + \zeta^{50} p^3 + \zeta^{13} p^4 + \zeta^{44} p^5 + \zeta^{24} p^6 + \zeta^{27} p^7 + \zeta^{24} p^8 + \zeta^{19} p^9 + \dots$$

Again we have a constant product:

$$\prod_{1 \leq i \leq 6} \tau(m, \zeta^0 + \zeta^1, \mathfrak{p}_i) = \zeta^3$$

for all  $m \geq 0$  when the product is nonzero. However, observe that for  $i = 1, 2, 3$ ,

$$\tau(m, \zeta^0 + \zeta^1, \mathfrak{p}_i) \tau(m, \zeta^0 + \zeta^1, \mathfrak{p}_{7-i}) = \zeta^1.$$

These pairwise products refine the collusion noted between all 6 primes. This may lead us to expect collusions to come in pairs, but the next example shows collusion in triples of primes:

$$\mathbf{p}_1 : \zeta^4 + \zeta^{37} + \zeta^{43} = \zeta^{56} + \zeta^{35}p + \zeta^{56}p^2 + \zeta^{14}p^3 + \zeta^{14}p^4 + \zeta^{35}p^5 + \zeta^{35}p^6 + \zeta^{56}p^7 + \zeta^{14}p^8 + \dots$$

$$\mathbf{p}_2 : \zeta^4 + \zeta^{37} + \zeta^{43} = \zeta^{35} + \zeta^{14}p + \zeta^{35}p^2 + \zeta^{56}p^3 + \zeta^{56}p^4 + \zeta^{14}p^5 + \zeta^{14}p^6 + \zeta^{35}p^7 + \zeta^{56}p^8 + \dots$$

$$\mathbf{p}_3 : \zeta^4 + \zeta^{37} + \zeta^{43} = \zeta^{14} + \zeta^{56}p + \zeta^{14}p^2 + \zeta^{35}p^3 + \zeta^{35}p^4 + \zeta^{56}p^5 + \zeta^{56}p^6 + \zeta^{14}p^7 + \zeta^{35}p^8 + \dots$$

$$\mathbf{p}_4 : \zeta^4 + \zeta^{37} + \zeta^{43} = \zeta^{35} + \zeta^{35}p + \zeta^{56}p^2 + \zeta^{14}p^3 + \zeta^{35}p^4 + 0p^5 + 0p^6 + \zeta^{35}p^7 + \zeta^{14}p^8 + \dots$$

$$\mathbf{p}_5 : \zeta^4 + \zeta^{37} + \zeta^{43} = \zeta^{56} + \zeta^{56}p + \zeta^{14}p^2 + \zeta^{35}p^3 + \zeta^{56}p^4 + 0p^5 + 0p^6 + \zeta^{56}p^7 + \zeta^{35}p^8 + \dots$$

$$\mathbf{p}_6 : \zeta^4 + \zeta^{37} + \zeta^{43} = \zeta^{14} + \zeta^{14}p + \zeta^{35}p^2 + \zeta^{56}p^3 + \zeta^{14}p^4 + 0p^5 + 0p^6 + \zeta^{14}p^7 + \zeta^{56}p^8 + \dots$$

Here we have constant triple products for  $\alpha = \zeta^4 + \zeta^{37} + \zeta^{43}$  and  $i = 1, 4$ :

$$\tau(m, \alpha, \mathbf{p}_i)\tau(m, \alpha, \mathbf{p}_{i+1})\tau(m, \alpha, \mathbf{p}_{i+2}) = \zeta^{42}.$$

Furthermore,  $\zeta^4 + \zeta^{37} + \zeta^{43}$  gives another example of the restricted coefficient phenomenon, since  $\{0, \zeta^{14}, \zeta^{35}, \zeta^{56}\}$  are the only coefficients appearing in any of these expansions. Note that in all cases we have seen of the restricted coefficients phenomenon, the total number of permissible Teichmüller representatives has been a power of  $p$ .

The remainder of the paper is divided into three sections. Section 3 reviews background on cyclotomic fields. Section 4 develops theory which we use in Section 5 to explain the permutation conspiracy, restricted coefficients phenomenon, and prime collusion. All three are related to the dynamics of an affine group action on  $\mathbb{Z}[\zeta]$  established in Theorem 3.

### 3. BACKGROUND

We review the basic theory of cyclotomic fields. Proofs may be found in Lang [3, Chp. IV]. To begin, the polynomial  $x^n - 1$  factors in  $\mathbb{Z}[x]$  as

$$x^n - 1 = \prod_{d|n} \Phi_d(x),$$

where  $\Phi_d(x)$  is an irreducible polynomial of degree  $\varphi(d)$  called the *dth cyclotomic polynomial*. Recall that  $\varphi(d) = |(\mathbb{Z}/(d))^\times|$  is Euler's totient function. The roots of  $\Phi_n(x)$  are primitive  $n$ th roots of unity: algebraic integers  $\zeta$  such that  $\zeta^n = 1$  and  $\zeta^d \neq 1$  for any proper divisor  $d | n$ . If  $\zeta$  is a primitive  $n$ th root of unity and  $a$  is an integer coprime to  $n$ , then  $\zeta^a$  is again a primitive  $n$ th root of unity. Furthermore, every primitive  $n$ th root of unity may be expressed as  $\zeta^a$  for some  $a$  with  $(a, n) = 1$ . Therefore  $\Phi_n(x)$  splits completely in  $\mathbb{Q}(\zeta)$  and  $\mathbb{Q}(\zeta)/\mathbb{Q}$  is a Galois extension of degree  $\varphi(n)$  with Galois group canonically isomorphic to  $(\mathbb{Z}/(n))^\times$ . We use this isomorphism frequently without further comment, writing  $\alpha^\sigma$  to denote the action of  $\sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  but also viewing  $\sigma$  as a unit modulo  $n$  as in  $\zeta^\sigma$ .

If  $p$  is a prime, then  $\Phi_n(x)$  is typically not irreducible in  $\mathbb{Z}_p[x]$ . By Hensel's lemma [4, Lem. 4.6], the factorization is determined by the orbits of Frobenius on the primitive  $n$ th roots of unity. If  $(n, p) = 1$ , then  $p \in (\mathbb{Z}/(n))^\times \cong \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$  and the size of the orbits of Frobenius on the primitive  $n$ th roots of unity is the same as the multiplicative order of  $p$  modulo  $n$ . That is, if  $d > 0$  is minimal such that  $p^d \equiv 1 \pmod{n}$ , then  $\Phi_n(x)$  factors into  $\varphi(n)/d$  irreducible degree  $d$  polynomials in  $\mathbb{Z}_p[x]$ . The case of interest to us is when  $n = q - 1 = p^d - 1$ . With  $n$  written in this form it is clear that  $(n, p) = 1$  and  $d$  is the multiplicative order of  $p$  modulo  $n$ .

The *affine group*  $\text{Aff}(n)$  is defined by

$$\text{Aff}(n) = \{\sigma x + b : \sigma \in (\mathbb{Z}/(n))^\times, b \in \mathbb{Z}/(n)\},$$

where the elements are considered as linear functions in the formal variable  $x$  and the group operation is composition of functions:

$$(\sigma_1 x + b_1) \circ (\sigma_2 x + b_2) = \sigma_1(\sigma_2 x + b_2) + b_1 = (\sigma_1 \sigma_2)x + (\sigma_1 b_2 + b_1).$$

Another way to view  $\text{Aff}(n)$  is as a semidirect product

$$\text{Aff}(n) \cong \mathbb{Z}/(n) \rtimes (\mathbb{Z}/(n))^\times.$$

If  $H \subseteq (\mathbb{Z}/(n))^\times$  is a subgroup, then  $\text{Aff}(H) \subseteq \text{Aff}(n)$  is the subgroup

$$\text{Aff}(H) = \{\sigma x + b \in \text{Aff}(n) : \sigma \in H\}.$$

There is a  $\mathbb{Z}$ -linear action of  $\text{Aff}(n)$  on  $\mathbb{Z}[\zeta]$  given by

$$\sigma x + b : \alpha \mapsto \alpha^\sigma \zeta^b.$$

In particular, if  $\alpha = \zeta^a$ , then  $(\sigma x + b)\zeta^a = \zeta^{\sigma a + b}$ .

If  $n = q - 1 = p^d - 1$ , let  $H_p \subseteq (\mathbb{Z}/(q - 1))^\times$  be the subgroup generated by  $p$ . If  $\mathfrak{p}$  is a prime in  $\mathbb{Z}[\zeta]$  over  $p$ , then  $(p^c x + b)\mathfrak{p} = \mathfrak{p}$  for each  $p^c x + b \in \text{Aff}(H_p)$  since  $H_p$  is the decomposition group of each  $\mathfrak{p}$  over  $p$ .

In Section 4 we are interested in the number of fixed points of an element  $p^c x + b \in \text{Aff}(H_p)$  in  $\mu_{q-1} \cup \{0\}$ . We determine this in Proposition 2. First, a lemma.

**Lemma 1.** *There exist polynomials  $f(x), g(x) \in \mathbb{Z}[x]$  such that*

$$f(x) \frac{x^a - 1}{x - 1} + g(x) \frac{x^b - 1}{x - 1} = \frac{x^{(a,b)} - 1}{x - 1}. \quad (1)$$

*It follows that for any integer  $m$  we have*

$$(m^a - 1, m^b - 1) = m^{(a,b)} - 1. \quad (2)$$

*Proof.* If  $a = qb + r$  with  $0 \leq r < b$ , then

$$\frac{x^a - 1}{x - 1} = (x^{a-b} + x^{a-2b} + \dots + x^{a-qb}) \frac{x^b - 1}{x - 1} + \frac{x^r - 1}{x - 1}.$$

Thus we can follow the usual Euclidean algorithm to get the desired polynomial identity (1). Dividing (1) by  $(x^{(a,b)} - 1)/(x - 1)$  we have

$$f(x) \frac{x^a - 1}{x^{(a,b)} - 1} + g(x) \frac{x^b - 1}{x^{(a,b)} - 1} = 1$$

in  $\mathbb{Z}[x]$ . Evaluating at  $x = m$  we deduce

$$\left( \frac{m^a - 1}{m^{(a,b)} - 1}, \frac{m^b - 1}{m^{(a,b)} - 1} \right) = 1.$$

Multiplying by  $m^{(a,b)} - 1$  yields the identity (2).  $\square$

**Proposition 2.** *The element  $p^c x + b \in \text{Aff}(H_p)$  has fixed points in  $\mu_{q-1}$  iff  $p^{(c,d)} - 1 \mid b$ , and in that case it has precisely  $p^{(c,d)} - 1$  fixed points in  $\mu_{q-1}$ . Since 0 is always fixed, it follows that the total number of fixed points in  $\tau(\mathbb{F}_q) = \mu_{q-1} \cup \{0\}$  is  $p^{(c,d)}$ .*

*Proof.* If  $\zeta^a$  is a fixed point of  $p^c x + b$ , then  $p^c a + b = a$  hence  $(p^c - 1)a + b = 0$  in  $\mathbb{Z}/(q - 1)$ . Let  $g = p^{(c,d)} - 1$ . Then  $g = (p^c - 1, p^d - 1)$  by Lemma 1. Reducing  $(p^c - 1)y + b = 0$  modulo  $g$  we conclude that  $g \mid b$ .

Supposing  $g \mid b$ , the linear equation  $\frac{p^c - 1}{g}x + \frac{b}{g} = 0$  has a unique solution modulo  $\frac{q-1}{g}$  which lifts to  $g$  distinct solutions modulo  $q - 1$ . Thus  $p^c x + b$  has a total of  $g + 1 = p^{(c,d)}$  fixed points in  $\mu_{q-1} \cup \{0\}$ .  $\square$

#### 4. THEORY

The Teichmüller expansion of  $\alpha$  at  $\mathfrak{p}$  is defined locally as an infinite sum which does not converge in the global ring  $\mathbb{Z}[\zeta]$ . Nevertheless, Theorem 3 shows that the global Galois group acts nicely on Teichmüller expansions.

Recall our definition of the affine group  $\text{Aff}(n)$  and its subgroup  $\text{Aff}(H_p)$  assuming  $(n, p) = 1$ ,

$$\begin{aligned}\text{Aff}(n) &= \{\sigma x + b : \sigma \in (\mathbb{Z}/(n))^\times, b \in \mathbb{Z}/(n)\} \\ \text{Aff}(H_p) &= \{p^c x + b \in \text{Aff}(n) : c \geq 0\}.\end{aligned}$$

**Theorem 3.** *Let  $\zeta$  be a primitive  $(q - 1)$ th root of unity. Suppose  $\mathfrak{p} \subseteq \mathbb{Z}[\zeta]$  is a prime over  $p$ , and  $\alpha \in \mathbb{Z}[\zeta]$ . If  $\sigma x + b \in \text{Aff}(n)$ , then*

$$(\sigma x + b)\tau(m, \alpha, \mathfrak{p}) = \tau(m, (\sigma x + b)\alpha, \mathfrak{p}^\sigma).$$

*In other words, if*

$$\alpha = \tau(0, \alpha, \mathfrak{p}) + \tau(1, \alpha, \mathfrak{p})p + \tau(2, \alpha, \mathfrak{p})p^2 + \dots$$

*is the Teichmüller expansion of  $\alpha$  at  $\mathfrak{p}$ , then*

$$(\sigma x + b)\alpha = (\sigma x + b)\tau(0, \alpha, \mathfrak{p}) + (\sigma x + b)\tau(1, \alpha, \mathfrak{p})p + (\sigma x + b)\tau(2, \alpha, \mathfrak{p})p^2 + \dots$$

*is the Teichmüller expansion of  $(\sigma x + b)\alpha$  at  $\mathfrak{p}^\sigma$ .*

*Proof.* Let  $\alpha(m, \mathfrak{p})$  be the sum of the first  $m$  terms of the Teichmüller expansion of  $\alpha$  at  $\mathfrak{p}$ . Then

$$\alpha(m, \mathfrak{p}) = \sum_{k < m} \tau(k, \alpha, \mathfrak{p})p^k$$

is the unique element of  $\mathbb{Z}[\zeta]$  which may be written as a polynomial in  $p$  of degree less than  $m$  with coefficients in  $\tau(\mathbb{F}_q) = \mu_{q-1} \cup \{0\}$  such that  $\alpha - \alpha(m, \mathfrak{p}) \in \mathfrak{p}^m$ . If  $\sigma \in \text{Gal}(\mathbb{Q}(\zeta)/\mathbb{Q})$ , then  $\alpha^\sigma \zeta^b - \alpha(m, \mathfrak{p})^\sigma \zeta^b \in (\mathfrak{p}^\sigma)^m$ . Since  $p \in \mathbb{Z}$  is fixed by  $\sigma$  we have

$$(\sigma x + b)\alpha(m, \mathfrak{p}) = \alpha(m, \mathfrak{p})^\sigma \zeta^b = \sum_{k < m} \tau(k, \alpha, \mathfrak{p})^\sigma \zeta^b p^k,$$

which is a polynomial in  $p$  of degree less than  $m$  with coefficients in  $\tau(\mathbb{F}_q)$ . Hence

$$(\sigma x + b)\alpha(m, \mathfrak{p}) = \alpha^\sigma(m, \mathfrak{p}^\sigma)\zeta^b$$

by uniqueness. This implies that  $(\sigma x + b)\tau(m, \alpha, \mathfrak{p}) = \tau(m, (\sigma x + b)\alpha, \mathfrak{p}^\sigma)$  for each  $m \geq 0$ .  $\square$

To summarize Theorem 3, the affine group  $\text{Aff}(n)$  acts coordinatewise on Teichmüller expansions while permuting the primes  $\mathfrak{p}$  over  $p$ .

Next we deduce three results using Theorem 3 to explain the permutation conspiracy, restricted coefficient phenomenon, and prime collusion in Section 5. Proposition 4 applies to the permutation conspiracy.

**Proposition 4.** *If  $\alpha \in \mathbb{Z}[\zeta]$  and  $\sigma x + b \in \text{Aff}(H_p)$ , then*

$$\tau(m, (\sigma x + b)\alpha, \mathfrak{p}) = (\sigma x + b)\tau(m, \alpha, \mathfrak{p}).$$

*Hence the Teichmüller expansion of  $(\sigma x + b)\alpha$  at  $\mathfrak{p}$  is the same as that of  $\alpha$  at  $\mathfrak{p}$  up to a permutation of the coefficients fixing 0.*

*Proof.* By Theorem 3 we have

$$(\sigma x + b)\tau(m, \alpha, \mathfrak{p}) = \tau(m, (\sigma x + b)\alpha, \mathfrak{p}^\sigma) = \tau(m, (\sigma x + b)\alpha, \mathfrak{p}).$$

since  $\sigma = p^c$  fixes  $\mathfrak{p}$  (see Section 3). Note that every element of  $\text{Aff}(q-1)$  fixes 0 and the rest of the permutation claim follows from  $\tau(\mathbb{F}_q)$  being closed under the action of  $\text{Aff}(q-1)$ .  $\square$

Proposition 5 helps us understand the restricted coefficients phenomenon.

**Proposition 5.** *If  $\alpha \in \mathbb{Z}[\zeta]$  is invariant under  $p^c x + b \in \text{Aff}(H_p)$ , then the Teichmüller coefficients of  $\alpha$  at any prime  $\mathfrak{p}$  over  $p$  are fixed points of  $p^c x + b$ . If  $\alpha \neq 0$ , then  $p^{(c,d)} - 1 \mid b$  and there are  $p^{(c,d)}$  fixed points of  $p^c x + b$  in  $\tau(\mathbb{F}_q)$ .*

*Proof.* Theorem 3 implies that for  $\sigma = p^c$ ,

$$(\sigma x + b)\tau(m, \alpha, \mathfrak{p}) = \tau(m, (\sigma x + b)\alpha, \mathfrak{p}^\sigma) = \tau(m, \alpha, \mathfrak{p}),$$

so the Teichmüller coefficients of  $\alpha$  at  $\mathfrak{p}$  are fixed points of  $p^c x + b$ . If  $\alpha \neq 0$ , then there is some nonzero Teichmüller coefficient. Hence  $p^c x + b$  has fixed points in  $\mu_{q-1}$ . Proposition 2 tells us  $p^{(c,d)} - 1 \mid b$  and that the total number of fixed points in  $\tau(\mathbb{F}_q)$  is  $p^{(c,d)}$ .  $\square$

Finally, Proposition 6 explains prime collusion.

**Proposition 6.** *Suppose  $\alpha \in \mathbb{Z}[\zeta]$  is invariant under an element  $\sigma x + b \in \text{Aff}(q-1)$  of order  $k$ . Then for any  $m \geq 0$  and prime  $\mathfrak{p}$  over  $p$ ,*

- (1) *If  $\tau(m, \alpha, \mathfrak{p}) = 0$ , then  $\tau(m, \alpha, \mathfrak{p}^{\sigma^i}) = 0$  for all  $i \geq 0$ .*
- (2) *If  $\tau(m, \alpha, \mathfrak{p}) \neq 0$ , then*

$$\prod_{0 \leq i < k} \tau(m, \alpha, \mathfrak{p}^{\sigma^i}) = (ux + vb)\tau(m, \alpha, \mathfrak{p})$$

*where  $u, v$  are given by*

$$u \equiv \sum_{0 \leq i < k} \sigma^i \pmod{q-1} \quad v \equiv \sum_{0 \leq i < k} \sum_{1 \leq j \leq i} \sigma^j \pmod{q-1}$$

*Alternatively,  $u, v \in \mathbb{Z}/(q-1)$  are the unique elements such that for each maximal prime power divisor  $\ell^n \mid q-1$ ,*

- (a) *If  $\sigma \equiv 1 \pmod{\ell^n}$ , then*

$$u \equiv k \pmod{\ell^n} \quad v \equiv \frac{k(k+1)}{2} \pmod{\ell^n}$$

- (b) *If  $\sigma \not\equiv 1 \pmod{\ell^n}$  then*

$$u \equiv 0 \pmod{\ell^r} \quad (1 - \sigma)v \equiv k \pmod{\ell^r}$$

*where  $r = n - v_\ell(1 - \sigma)$  and  $v_\ell(a)$  denotes the normalized  $\ell$ -valuation of  $a$ .*



*Proof.* Let  $(\sigma x + b)^i$  denote the  $i$ th iterate of  $\sigma x + b$  in  $\text{Aff}(q - 1)$ . Then Theorem 3 implies that for each  $m \geq 0$

$$(\sigma x + b)^i \tau(m, \alpha, \mathfrak{p}) = \tau(m, (\sigma x + b)^i \alpha, \mathfrak{p}^{\sigma^i}) = \tau(m, \alpha, \mathfrak{p}^{\sigma^i}),$$

since  $\alpha$  is fixed by  $\sigma x + b$ . So (1) follows from 0 being fixed by  $\text{Aff}(q - 1)$ .

Now suppose  $\tau(m, \alpha, \mathfrak{p}) \neq 0$ . Then

$$\begin{aligned} \prod_{0 \leq i < k} \tau(m, \alpha, \mathfrak{p}^{\sigma^i}) &= \prod_{0 \leq i < k} (\sigma x + b)^i \tau(m, \alpha, \mathfrak{p}) \\ &= \prod_{0 \leq i < k} \tau(m, \alpha, \mathfrak{p})^{\sigma^i} \zeta^{\sum_{1 \leq j \leq i} \sigma^j b} \\ &= \tau(m, \alpha, \mathfrak{p})^{\sum_{0 \leq i < k} \sigma^i} \zeta^{\sum_{0 \leq i < k} \sum_{1 \leq j \leq i} \sigma^j b} \\ &= (ux + vb) \tau(m, \alpha, \mathfrak{p}), \end{aligned}$$

where

$$u \equiv \sum_{0 \leq i < k} \sigma^i \pmod{q - 1} \quad v \equiv \sum_{0 \leq i < k} \sum_{1 \leq j \leq i} \sigma^j \pmod{q - 1}.$$

Note that  $u$  may be 0 in which case we interpret the action of  $(ux + vb)$  as simply multiplication by  $\zeta^{vb}$ . It does not seem possible to find simple evaluations for these sums modulo  $q - 1$ , but we can do so modulo the maximal prime power divisors  $\ell^n \mid q - 1$  and then use the Chinese Remainder Theorem to show that these local computations uniquely determine  $u$  and  $v$ .

If  $\sigma \equiv 1 \pmod{\ell^n}$ , then the sums simplify to well-known values,

$$u \equiv k \pmod{\ell^n} \quad v \equiv \frac{k(k+1)}{2} \pmod{\ell^n}.$$

If  $\sigma \not\equiv 1 \pmod{\ell^n}$ , then

$$(1 - \sigma)u \equiv 1 - \sigma^k \equiv 0 \pmod{\ell^n},$$

which implies  $u \equiv 0 \pmod{\ell^r}$  with  $r = n - v_\ell(1 - \sigma)$ .

Next we compute

$$v = \sum_{0 \leq i < k} \sum_{1 \leq j \leq i} \sigma^j = \sum_{0 \leq j < k} \sum_{j \leq i < k} \sigma^j = \sum_{0 \leq j < k} (k - j) \sigma^j = ku - \sum_{0 \leq j < k} j \sigma^j,$$

where the first equality results from switching the order of summation and reindexing. Multiplying by  $1 - \sigma$  yields

$$(1 - \sigma)v = k(1 - \sigma)u - (1 - \sigma) \sum_{0 \leq j < k} j \sigma^j \equiv k + \sum_{0 \leq j < k} \sigma^j \equiv k + u \pmod{\ell^n}.$$

Multiplying by  $1 - \sigma$  again we have

$$(1 - \sigma)^2 v = (1 - \sigma)k \pmod{\ell^n}.$$

So  $(1 - \sigma)v \equiv k \pmod{\ell^r}$ . □

## 5. APPLICATION

We revisit the examples from Section 2, applying the results from Section 4 to explain the conspiracies and collusion.

**Permutation conspiracy.** Let  $q = p^d$  and let  $\zeta$  be a  $(q-1)$ th root of unity. Proposition 4 implies that the Teichmüller expansion at  $\mathfrak{p}$  of any element in the  $\text{Aff}(H_p)$  orbit of  $\alpha$  is a permutation of the Teichmüller expansion of  $\alpha$  at  $\mathfrak{p}$  fixing 0.

Recall these Teichmüller expansions at  $\mathfrak{p}_1 = (2, \zeta^4 + \zeta + 1)$  when  $q = 2^4$  from Section 2:

$$\begin{aligned}\zeta^0 + \zeta^1 &= \zeta^4 + \zeta^8 p + \zeta^6 p^2 + \zeta^5 p^3 + \zeta^3 p^4 + 0p^5 + \zeta^8 p^6 + \zeta^{10} p^7 + \zeta^7 p^8 + \zeta^{10} p^9 + \dots \\ \zeta^1 + \zeta^3 &= \zeta^9 + \zeta^2 p + \zeta^{13} p^2 + \zeta^{11} p^3 + \zeta^7 p^4 + 0p^5 + \zeta^2 p^6 + \zeta^6 p^7 + \zeta^0 p^8 + \zeta^6 p^9 + \dots \\ \zeta^2 + \zeta^{10} &= \zeta^4 + \zeta^6 p + \zeta^5 p^2 + \zeta^{12} p^3 + \zeta^{11} p^4 + 0p^5 + \zeta^6 p^6 + \zeta^7 p^7 + \zeta^{13} p^8 + \zeta^7 p^9 + \dots \\ \zeta^3 + \zeta^7 &= \zeta^4 + \zeta^5 p + \zeta^{12} p^2 + \zeta^8 p^3 + \zeta^0 p^4 + 0p^5 + \zeta^5 p^6 + \zeta^{13} p^7 + \zeta^1 p^8 + \zeta^{13} p^9 + \dots\end{aligned}$$

The permutation conspiracies are consequences of the following calculations:

$$(2x+1)(\zeta^0 + \zeta^1) = \zeta^1 + \zeta^3 \quad (8x+2)(\zeta^0 + \zeta^1) = \zeta^2 + \zeta^{10} \quad (4x+3)(\zeta^0 + \zeta^1) = \zeta^3 + \zeta^7$$

It's important to note that each element of  $\text{Aff}(15)$  above has the form  $2^c x + b$ .

The permutations are determined explicitly by the linear functions; applying  $2x+1$  to the exponents of the Teichmüller coefficients in  $\zeta^0 + \zeta^1$  yields the expansion of  $\zeta^1 + \zeta^3$  below it. The group  $\text{Aff}(H_2)$  has order  $d(q-1) = 4 \cdot 15 = 60$  and the element  $\zeta^0 + \zeta^1$  has a trivial stabilizer, thus an orbit with 60 elements. Therefore, of the  $\binom{q-1}{2} = 105$  sums of the form  $\zeta^a + \zeta^b$  with  $a \not\equiv b \pmod{15}$ , approximately 57% of them will be permutations of the expansion of  $\zeta^0 + \zeta^1$ . More generally for any  $q$ ,  $\zeta^0 + \zeta^1$  always has trivial stabilizer under  $\text{Aff}(H_p)$ , hence the proportion of  $\zeta^a + \zeta^b$  which are permutations of  $\zeta^0 + \zeta^1$  is

$$\frac{d(q-1)}{\binom{q-1}{2}} = \frac{2d}{q-2}.$$

We saw two periodic expansions

$$\begin{aligned}\zeta^1 + \zeta^6 &= \zeta^{11} + \zeta^{11} p + \zeta^{11} p^2 + \dots \\ \zeta^4 + \zeta^{14} &= \zeta^9 + \zeta^9 p + \zeta^9 p^2 + \dots\end{aligned}$$

which are related by  $(2x+2)(\zeta^1 + \zeta^6) = \zeta^4 + \zeta^{14}$ . The periodic expansion itself is special and can be understood by summing the geometric series which converges locally:

$$\zeta^1 + \zeta^6 = \zeta^{11} + \zeta^{11} p + \zeta^{11} p^2 + \dots = \zeta^{11} (1 + p + p^2 + \dots) = \frac{\zeta^{11}}{1-p} = -\zeta^{11}.$$

This identity is equivalent to  $\zeta^{10} + \zeta^5 + 1 = 0$ , telling us  $\zeta^5$  is a primitive 3rd root of unity.

**Restricted coefficients.** Our last example of the permutation conspiracy also exhibited the restricted coefficient phenomenon.

$$\begin{aligned}\zeta^0 + \zeta^3 &= \zeta^{14} + \zeta^9 p + \zeta^4 p^2 + \zeta^9 p^3 + \zeta^{14} p^4 + 0p^5 + 0p^6 + \zeta^9 p^7 + \zeta^{14} p^8 + 0p^9 + \dots \\ \zeta^2 + \zeta^{11} &= \zeta^9 + \zeta^{14} p + \zeta^4 p^2 + \zeta^{14} p^3 + \zeta^9 p^4 + 0p^5 + 0p^6 + \zeta^{14} p^7 + \zeta^9 p^8 + 0p^9 + \dots \\ \zeta^1 + \zeta^7 &= \zeta^{14} + \zeta^4 p + \zeta^9 p^2 + \zeta^4 p^3 + \zeta^{14} p^4 + 0p^5 + 0p^6 + \zeta^4 p^7 + \zeta^{14} p^8 + 0p^9 + \dots\end{aligned}$$

The permutations follow from

$$\begin{aligned}(8x+2)(\zeta^0 + \zeta^3) &= \zeta^2 + \zeta^{11} \\ (2x+1)(\zeta^0 + \zeta^3) &= \zeta^1 + \zeta^7.\end{aligned}$$

To see why the coefficients all belong to  $\{0, \zeta^4, \zeta^9, \zeta^{14}\}$ , notice that  $\zeta^0 + \zeta^3$  is invariant under  $4x + 3 \in \text{Aff}(H_2)$ . Proposition 4 says the coefficients of the Teichmüller expansions of  $\zeta^0 + \zeta^3$  at both primes  $\mathfrak{p}_1$  and  $\mathfrak{p}_2$  are invariant under  $4x + 3$ . The fixed points of  $4x + 3$  in  $\tau(\mathbb{F}_{16})$  are precisely  $\{0, \zeta^4, \zeta^9, \zeta^{14}\}$ . This set has  $2^{(2,4)} = 2^2$  elements, as predicted, since  $p^c x + b = 2^2 x + 3$  and  $d = 4$ .

**Prime collusion.** We observed that the product of the Teichmüller coefficients of  $\alpha \in \mathbb{Z}[\zeta]$  over certain groupings of primes were often independent of the index  $m$  and always restricted. For example, with  $q = 2^4$  we had

$$\begin{aligned} \mathfrak{p}_1 : \zeta^0 + \zeta^1 &= \zeta^4 + \zeta^8 p + \zeta^6 p^2 + \zeta^5 p^3 + \zeta^3 p^4 + 0 p^5 + \zeta^8 p^6 + \zeta^{10} p^7 + \zeta^7 p^8 + \zeta^{10} p^9 + \dots \\ \mathfrak{p}_2 : \zeta^0 + \zeta^1 &= \zeta^{12} + \zeta^8 p + \zeta^{10} p^2 + \zeta^{11} p^3 + \zeta^{13} p^4 + 0 p^5 + \zeta^8 p^6 + \zeta^6 p^7 + \zeta^9 p^8 + \zeta^6 p^9 + \dots \end{aligned}$$

Then  $\tau(m, \zeta^0 + \zeta^1, \mathfrak{p}_1) \tau(m, \zeta^0 + \zeta^1, \mathfrak{p}_2) = \zeta^1$  appears to be true for each  $m \geq 0$  when the product is not zero. To verify this, notice that  $\zeta^0 + \zeta^1$  is invariant under the order two element  $-x + 1 \in \text{Aff}(15)$ . Proposition 6 tells us

$$\tau(m, \zeta^0 + \zeta^1, \mathfrak{p}_1) \tau(m, \zeta^0 + \zeta^1, \mathfrak{p}_2) = (ux + vb) \tau(m, \zeta^0 + \zeta^1, \mathfrak{p}_1),$$

where  $u = 1 + \sigma = 0$  and  $v = 1 + (1 + \sigma) = 1$ . Hence,

$$\tau(m, \zeta^0 + \zeta^1, \mathfrak{p}_1) \tau(m, \zeta^0 + \zeta^1, \mathfrak{p}_2) = \zeta^{vb} = \zeta^1.$$

Since  $u = 0$ , the products are independent of  $m$ . Proposition 7 shows this is always the case for  $\alpha = \zeta^{a_1} + \zeta^{a_2}$ .

**Proposition 7.** *If  $\alpha = \zeta^{a_1} + \zeta^{a_2}$  with  $a_1 \not\equiv a_2 \pmod{q-1}$ , then  $\alpha$  is invariant under  $-x + a_1 + a_2$ . Let  $\bar{\mathfrak{p}} := \mathfrak{p}^\sigma$  when  $\sigma = -1$ . Then*

$$\tau(m, \alpha, \mathfrak{p}) \tau(m, \alpha, \bar{\mathfrak{p}}) = \zeta^{a_1 + a_2}.$$

*Proof.* Verifying the invariance of  $\alpha$  under  $-x + a_1 + a_2$  is straightforward. We apply Proposition 6 with  $\sigma = -1$  and  $k = 2$ . In this simple case we may evaluate the summations for  $u$  and  $v$  directly:  $u = 1 + \sigma = 0$  and  $v = 1 + (1 + \sigma) = 1$ . We conclude that when  $\tau(m, \alpha, \mathfrak{p}) \neq 0$ ,

$$\tau(m, \alpha, \mathfrak{p}) \tau(m, \alpha, \bar{\mathfrak{p}}) = (ux + v(a_1 + a_2)) \tau(m, \alpha, \mathfrak{p}) = \zeta^{a_1 + a_2}.$$

□

With  $q = 2^6$  we saw collusion in triplets of primes together with restricted coefficients.

$$\begin{aligned} \mathfrak{p}_1 : \zeta^4 + \zeta^{37} + \zeta^{43} &= \zeta^{56} + \zeta^{35} p + \zeta^{56} p^2 + \zeta^{14} p^3 + \zeta^{14} p^4 + \zeta^{35} p^5 + \zeta^{35} p^6 + \zeta^{56} p^7 + \zeta^{14} p^8 + \dots \\ \mathfrak{p}_2 : \zeta^4 + \zeta^{37} + \zeta^{43} &= \zeta^{35} + \zeta^{14} p + \zeta^{35} p^2 + \zeta^{56} p^3 + \zeta^{56} p^4 + \zeta^{14} p^5 + \zeta^{14} p^6 + \zeta^{35} p^7 + \zeta^{56} p^8 + \dots \\ \mathfrak{p}_3 : \zeta^4 + \zeta^{37} + \zeta^{43} &= \zeta^{14} + \zeta^{56} p + \zeta^{14} p^2 + \zeta^{35} p^3 + \zeta^{35} p^4 + \zeta^{56} p^5 + \zeta^{56} p^6 + \zeta^{14} p^7 + \zeta^{35} p^8 + \dots \end{aligned}$$

$$\begin{aligned} \mathfrak{p}_4 : \zeta^4 + \zeta^{37} + \zeta^{43} &= \zeta^{35} + \zeta^{35} p + \zeta^{56} p^2 + \zeta^{14} p^3 + \zeta^{35} p^4 + 0 p^5 + 0 p^6 + \zeta^{35} p^7 + \zeta^{14} p^8 + \dots \\ \mathfrak{p}_5 : \zeta^4 + \zeta^{37} + \zeta^{43} &= \zeta^{56} + \zeta^{56} p + \zeta^{14} p^2 + \zeta^{35} p^3 + \zeta^{56} p^4 + 0 p^5 + 0 p^6 + \zeta^{56} p^7 + \zeta^{35} p^8 + \dots \\ \mathfrak{p}_6 : \zeta^4 + \zeta^{37} + \zeta^{43} &= \zeta^{14} + \zeta^{14} p + \zeta^{35} p^2 + \zeta^{56} p^3 + \zeta^{14} p^4 + 0 p^5 + 0 p^6 + \zeta^{14} p^7 + \zeta^{56} p^8 + \dots \end{aligned}$$

The element  $\alpha = \zeta^4 + \zeta^{37} + \zeta^{43}$  is invariant under the order three subgroup generated by  $16x + 42 \in \text{Aff}(H_2)$ . The fixed points of  $16x + 42$  are  $\{0, \zeta^{14}, \zeta^{35}, \zeta^{56}\}$ , hence the restricted coefficients

in the expansions above by Proposition 5. The collusion in the triplets is caused by the invariance of  $\alpha$  under the order three element  $25x + 0$ . Using Proposition 6 we compute

$$u \equiv 1 + 25 + 25^2 \equiv 21 \pmod{63} = q - 1.$$

The value of  $v$  is irrelevant since  $b = 0$ . Hence

$$\tau(m, \alpha, \mathfrak{p})\tau(m, \alpha, \mathfrak{p}^\sigma)\tau(m, \alpha, \mathfrak{p}^{\sigma^2}) = \tau(m, \alpha, \mathfrak{p})^{21}.$$

Since  $21a \equiv 42 \pmod{63}$  for  $a = 14, 35, 56 \equiv 2 \pmod{3}$  we conclude that

$$\tau(m, \alpha, \mathfrak{p})\tau(m, \alpha, \mathfrak{p}^\sigma)\tau(m, \alpha, \mathfrak{p}^{\sigma^2}) = \zeta^{42}$$

whenever  $\tau(m, \alpha, \mathfrak{p}) \neq 0$ .

**Conclusion.** Permutation conspiracies, restricted coefficient phenomena, and prime collusions are three readily apparent and seemingly unrelated patterns emerging in the Teichmüller expansions of sums of roots of unity. All three are consequences of the linear action of the affine group  $\text{Aff}(q - 1)$  on  $\mathbb{Z}[\zeta]$ : permutation conspiracies occur between elements in the same orbit under an element of  $\text{Aff}(H_p)$ ; restricted coefficients occur for elements fixed under some element of  $\text{Aff}(H_p)$ ; and prime collusions occur for elements fixed under a general element of  $\text{Aff}(q - 1)$ .

**Acknowledgements.** The author thanks Bob Lutz for helpful feedback on this manuscript.

#### REFERENCES

- [1] Hazewinkel, Michiel. “Witt vectors. part 1.” Handbook of algebra 6, 2009. 319-472.
- [2] Lang, Serge. Algebra. Vol. 211. Springer Science & Business Media, 2002.
- [3] Lang, Serge. Algebraic number theory. Vol. 110. Springer Science & Business Media, 2013.
- [4] Neukirch, Jürgen. Algebraic number theory. Vol. 322. Springer Science & Business Media, 2013.
- [5] Serre, Jean-Pierre. Local fields. Vol. 67. Springer Science & Business Media, 2013.

DEPT. OF MATHEMATICS, UNIVERSITY OF MICHIGAN, ANN ARBOR, MI 48109-1043,  
*E-mail address:* tghyde@umich.edu